The Latest Scams

223 E. Blackstock Road
Spartanburg, SC 29301

p. 864 582 7766
1-800-277-0025

asknoel@theprovestperspective.com
www.TheProvestPerspective.com
www.ProVestWealth.com

1. **Check Fraud.** Fraudsters are stealing other people's checks out of the mail and cashing them. One of the main ways fraudsters do this is by obtaining mailbox keys. Criminals have also assaulted mail carriers to steal mail directly from them, including checks. The Federal Deposit Insurance Corporation (FDIC) even flagged check fraud as a rising risk for banks in its *2024 Risk Report.* The FBI and U.S. Postal Investigative Service also issued a warning on 27 January 2025 that check fraud is rising—nearly doubling from 2021 to 2023.

   Fraudsters take advantage of regulations requiring financial institutions to make check funds available within specified timeframes, which is often too short a window for the consumer or financial institutions to identify and stop the fraud. As a result, the compromised checks clear, and the funds are withdrawn by the criminal participants before the fraud is detected.

2. **Cryptocurrency scams.** Cryptocurrency is hot, with the price of one Bitcoin reaching $100,000 for the first time in December 2024. That may be good for savvy investors, but the hype could lure novices into cryptocurrency scams — with huge potential losses. In 2023, the FBI's Internet Crime Complaint Center received nearly 9,000 cryptocurrency complaints from people age 50-59. Their total losses were more than $900 million. People age 60 and older registered nearly 17,000 complaints and reported losses of $1.6 billion. Scammers use dating apps, messaging apps, social media and other communications to build relationships and trust with their targets, then share their "expertise" on investments, frequently promising large returns and little risk. In 2023, this "confidence-enabled cryptocurrency investment fraud"

was the most prominent type of crypto scam, FBI reports. Criminals often show victims fake profit reports, which encourages them to invest more. But when investors try to withdraw funds, they're frequently charged outrageous fees. The bogus companies then typically vanish before investors receive their money.

If you're interested in crypto but lack expertise, talk with a financial advisor. And watch for impostor sites that mimic actual companies. In California, one victim transferred over $127,000 to two crypto exchanges, one of which was Celestia.bet. The true network, however, is Celestia.org. To confirm that a company is legit, make sure it's registered with the Commodities Futures Trading Commission and the National Futures Association. Also avoid companies with no physical address or customer service line.

3. **Tech support scams.** Consumers age 60 and older are five times more likely than their younger counterparts to lose money to tech support scams, which cost older Americans more $175 million in 2023, the FTC reported to Congress in October 2024. The fraud frequently starts with a pop-up message — often with a logo from companies like Microsoft or Apple — saying your computer has a virus. You click a link or call a supposed support number, and they request remote access to your computer. The criminals can now access all of the information on your machine and also install malware. The scammers may also try to sell you useless software, maintenance or warranty programs. In March 2024, the FTC reached a $26 million settlement with two tech-support companies who used fake Microsoft pop-ups to lure

consumers into buying software. Or they may install malware to harvest login credentials to your online accounts, including financial accounts.

Legitimate tech companies won't call, email, or text about problems with your computer, and their pop-ups will never ask you to make a call or click a link. If a tech support person calls you unexpectedly, it's almost surely a scam. Hang up, even if the number looks real. Never click on a pop-up, never give remote access to someone who calls you out of the blue, and never share your password. If the pop-up won't go away, restart your computer. If you do share your password, change it immediately. And if you give someone remote access to your computer, update your security software and run a scam, or have a trusted person or big box tech store scan it for you.

4. **Card-declined scams,** The BBB's Scam Tracker has received many recent reports from consumers whose credit cards are declined while making an online purchase. Typically they try using a different card, but that one fails, too. And yet despite the card-declined notices, the charges have actually occurred for each transaction — and often for more than they thought. After her card was denied, one victim tried it a second time, and received the same card-declined message. Then her credit card company alerted her that it had declined a $2,500 charge — even though she hadn't made a $2,500 charge while struggling with her transaction. There has been a noticeable increase in card-declined problems.

The fraud typically occurs when people visit fraudulent sites or click on fraudulent links. In September 2024, the American Automobile Association (AAA) warned its members about emails and texts (which appeared to come from AAA customer service) offering a free AAA car emergency kit if people took a survey. The catch: You had to pay for shipping. So people entered their credit card info and then received the card-declined message. One victim told AAA he found several fraudulent charges on his two credit cards.

To avoid this, always use a credit card rather than a debit card, because credit cards offer stronger fraud protections. If you're unfamiliar with a company, research it before making a purchase. And make sure a website is genuine. Scammers often build lookalike sites, so scrutinize the URL. Sometimes a letter or two might be different. Most importantly, if you receive an unsolicited offer, ignore it.

5. **AI Scams.** The clearest example of scammers using new technology comes from the explosion of artificial intelligence and thus AI-powered scams. In December 2024, the FBI posted a public service announcement listing some of the ways that criminals use generative AI to trick victims. There is an increasing role of generative AI in scams around the world and deepfake-related crime increased by more than 1,500% in the Asia-Pacific region from 2022 to 2023. Generative AI tools generally get classified by the type of content they generate, such as text, images or videos. Scammers can use them to enhance different types of popular scams:

- Phishing and smishing: Scammers can use AI to write more convincing and natural-sounding phishing emails and text messages.
- AI images: Scammers can use AI-generated images to quickly create eye-catching websites, social media ads, fake identification documents, explicit photos and fake headshots for social media profiles.
- Deepfake videos: AI-generated videos might be created to promote fake products, services or investments. Scammers also might use deepfake recordings or real-time face- and body-swapping tools to trick victims into thinking they're someone else.
- Fake and cloned voices: Scammers also use AI-generated or altered voices for their videos and for phone-based scams. Some AI tools can even mimic real accents. The potential to create an image, video or voice of someone can make many existing scams more believable, and it opens up new opportunities for scammers.

6. Imposter Scams. Scammers almost always hide their identity, and imposter scams are one of the most common types of scams or fraud because the category is fairly broad. These happen when the scammer pretends to be a friend, relative, celebrity, politician, businessperson, government agent, delivery person or company representative.

Now that scammers can use AI, it's more important than ever to be skeptical when someone contacts you, especially if they try to scare you or offer you a gift or investment opportunity.

Email and Text are the Preferred Contact Methods. The FTC reports that the percentage of imposter scams that start with a phone call has decreased from 67% in 2020 to 32% in 2023. Text messages and email are becoming a preferred method of first contact.

For example, the scammers might impersonate a company and send a message or email about a fake security alert, renewal, invoice, discount or tracking error. There are even multi-party scams, where the first scammer directs you to an accomplice who poses as a government agent or bank employee.

7. **Romance Scams.** While romance scams aren't new, a new twist on these are a prime example of how scammers can use generative AI to trick victims. Scammers often steal someone's identity or create fake profiles on dating and social media apps to meet victims. There's no surefire method to detect a fake. Some will use AI to deepfake video calls, and some crime organizations even force people or hire models to conduct romance scams. After gaining your trust, the scammer might ask you to buy them something, ask for money or give you an investment "tip" that's part of the scam. Or, the person may "mistakenly" send you money and ask you to send it back or forward it to someone else. If your bank later determines that their payment was fraudulent, the sum of the payment will be subtracted from your account. Many romance scams start with text messages, private messages on social media or in dating apps. Some scammers even seek to form platonic rather than romantic relationships.

8. **"Accidental" Text Messages.** Have you gotten a text message that seems genuine, but it also appears to be intended for someone else? It might say something like, "Sorry I'm running late, I'll be there in 15 minutes." Not wanting to be rude, you respond to tell the sender they've got the wrong number. These wrong number texts are often the first step in a romance or employment scam. Although there's sometimes a scammer on the other end from the start, scammers can also use AI messaging bots to target thousands of people at a time.

9. **Phone-Related Scams.** Scammers may contact you by phone, and some phone scams rely on smartphones' capabilities to access the internet and install malware. These phone-related scams include:

- Robocalls which have people's phones ringing nonstop with increasingly natural-sounding recorded voices. They may offer everything from auto warranties to vacations, or issue a threat to try and get your attention. Some robocalls can even respond to your questions using prerecorded or AI-generated messages.
- Malicious apps: Scammers may try to get you to install a malicious app to steal your information. Or, they might create a nearly identical copy of an existing app and then make money from in-app purchases. Recently, there were reports of malware that could infect your phone and trick you into calling the scammer when you try to call your bank.

- QR codes: These convenient codes have gained popularity as a touchless option to do things like read a restaurant menu or make a payment. However, scammers place their QR codes in inconspicuous spots, and scanning the code could prompt you to make a small purchase or enter your credentials on a lookalike website. Some scammers even go as far as printing QR codes on letters that appear to come from government agencies and then mailing them out.
- SIM swapping: This technique is used by a thief to reassign your number to a SIM card in a phone they control. They can then try to log in to your accounts using codes or links sent to your phone number. Contact your carrier to see if there are any security measures for stopping SIM swapping. Also, see if your accounts let you use a non SMS multifactor authentication option, such as an authenticator app that the scammer can't steal or access.
- One-time password (OTP) bots: Some scammers use so-called OTP bots to trick people into sharing the authentication codes. The scammer might try to log in, prompting the bank to send you a one-time code. At the same time, the bot imitates the company and calls, texts or emails you asking for the code. The timing might convince you that the bot's request is legitimate. However, if you respond, it sends the code to the scammer, who can now log in to your account.

10. **Online Purchase Scams.** Online purchase scams continue to be one of the riskiest types of scams, according to the Better Business Bureau. Although median losses were relatively low at $100, over 40% of the scams reported to the BBB were online purchase scams and over 80% of people report falling for the scam. Some scammers set up fake e-commerce stores and buy ads for the website on social media. Alternatively, scammers might list items for sale on online marketplaces, including social media platforms' marketplaces. The scammers might take your money and never send anything in return. Or, they might be committing triangulation fraud and purchasing the item you bought with someone else's stolen credit card. You might not realize you were part of a scam unless you try to return the item or use a warranty. Always look for red flags such as too-good-to-be-true prices, lack of details or high-pressure sales tactics. Paying with your credit card can also help you limit potential losses, as you can initiate a chargeback if you don't receive a product or service.

11. **Refund Phishing.** Some scammers figured out a new way to profit from stolen credit card information. Rather than focusing on stealing money from the card, they make a fraudulent purchase from a fake merchant whose name is a phone number or email. Victims call or visit the site to dispute the transaction, but they're phished—tricked into sharing personal and account information with the scammer.

12. Employment Scams. Employment scams use enticing, and hard-to-detect, lures to target people who've been out of work. Some scammers take a slow approach with interviews and a legitimate-seeming operation. They then collect personal information from your employment forms, or tell you to buy equipment or training. Other scams get right to the point and promise guaranteed or easy income—if you purchase their program. Sometimes, a fake employer sends a large paycheck and asks you to send the "extra" back—a play on the popular overpayment scam. The FTC says reports about task scams, when you're hired to repeat simple tasks online, increased from about 5,000 during all of 2023 to 20,000 during the first half of 2024. You might be able to withdraw small amounts at first. But the scam occurs when you're told you can pay to increase your earning rate and that you have to deposit money to unlock larger withdrawals. You make the payments, but you can't get any of the money—or your supposed earnings—out. You may also come across job opportunities that involve receiving money and sending funds to another account, or receiving and reshipping packages. These "money mule" and "reshipping mule" jobs are often part of an illegal operation, and you could be personally liable.

How to Avoid a Scam

While scammers' delivery methods and messaging can quickly change, a few basic security measures can help protect you from the latest and most common scams:

- Be skeptical when someone contacts you. Scammers can spoof calls and emails to make it look like they are coming from different sources, including government agencies, charities, banks and large companies. Don't share personal information, usernames, passwords or one-time codes that others can use to access your accounts or steal your identity.
- Don't click unknown links. Whether the link arrives in your email, a text or a direct message, never click on it unless you're certain the sender has good intentions. If the message says it's from a company or government agency, call the company using a number that you look up on your own to confirm its legitimacy.
- Be careful with your phone. Similarly, if you suspect a spam call, don't respond or press a button. The safest option is to hang up or ignore the call entirely. You can look up the organization and initiate a call if you're worried there may be an issue.
- Update your devices. Software updates may include important security measures that can help protect your phone, tablet or computer.
- Enable multifactor authentication. Add this feature to any accounts that offer it as an option, and try to use a non-SMS version to protect yourself from SIM swapping.
- Research companies before taking any actions. Before you make a purchase or donation, take a few minutes to review the company. Do a web search for its name plus "scam" or

"reviews" and research charities on Charity Navigator and CharityWatch.

- Don't refund or forward overpayments. Be careful whenever a company or person asks you to refund or forward part of a payment. Often, the original payment will be fraudulent and taken back later.
- Look for suspicious payment requirements. Scammers often ask for payments via cash, wire transfer, money order, cryptocurrency or gift cards. These payments can be harder to track and cancel than other forms of payment, which can leave you stuck without recourse.
- Create a family password. Create a family password that you can all use to verify that it's really one of you on the phone, and not someone who created a deepfaked video or cloned voice.

What to Do if You Fall Victim to a Scam

Although there are some exceptions, you often can't get your money back if you fall for a scam. There's also no way to take back any personal information that you sent. But there are a few steps you can take that might help prevent additional fraud and protect other people:

Report the scam and scammer. You can report scammers to the BBB and the FTC online. Additionally, report the scam and related message to any relevant parties, such as your bank, credit card issuer, social media platform, email provider, phone carrier or the USPS' Postal Inspection Service.

You can also file a police report, which might help with recovering your identity or lost funds.

- **Scan your devices.** If you clicked on a link or attachment, you may want to run an antivirus scan to check for malware.

- **Change your passwords.** Change the passwords on any accounts that use a password the scammer might know. Use this as an opportunity to create stronger passwords or try out the newer passwordless option called passkeys that are available on some websites.
- **Protect your credit.** You may be worried about identity theft if you gave the scammer your personal information. You have the right to add fraud alerts and security freezes, also called credit freezes, to your credit reports for free. These can help keep someone else from opening an account using your information.

ProVest Wealth Advisors / 223 East Blackstock Rd Spartanburg, SC 29301 / 800-277-0025 or 864-582-7766